APPLICATION
FOR
UNITED STATES LETTERS PATENT

TITLE: **Global Compliance System**

APPLICANT: **Frederic Greenbaum**
Michael Cortese
Waikit Ng

CERTIFICATE OF EXPRESS MAILING

EXPRESS MAIL Mailing Label Number EL785783845US

Date of Deposit: March 4, 2002

I hereby certify under 37 CFR 1.10 that this correspondence is being deposited with the United States Postal Service as "Express Mail Post Office to Addressee" with sufficient postage on the date indicated above and is addressed to the Commissioner for Patents, Washington, D.C. 20231.

Name: Melissa Scanzillo

Signature: Melissa Scanzillo

Clifford Chance Rogers & Wells LLP

GLOBAL COMPLIANCE SYSTEM

CROSS-REFERENCE TO RELATED APPLICATION

This application claims the benefit of the filing date of U.S. Provisional Application serial number 60/289,975 entitled "Global Compliance System" which was filed on May 10, 2001.

BACKGROUND

The following invention relates to compliance systems and, in particular, to a system for implementing a compliance program in a geographically-dispersed financial institution.

United States securities laws and the laws of other nations make it unlawful, in some circumstances, for a person who possesses non-public, material information about an issuer ("inside information") of publicly traded securities to trade in the securities without disclosing the information to the counterparty, or to "tip" others to the information. Broker dealers that engage in investment banking including both public underwriting and financial advice to public companies in mergers and acquisitions transactions often receive inside information. As a result they would be disabled from proprietary trading, including market making, publishing research, giving investment recommendations and managing money unless there were an effective way to prevent those engaged in those activities from learning about the inside information, as well as legal recognition of such policies and procedures to prevent attribution of the inside information to the broker dealer's traders, research analysts, portfolio manager and sales personnel even in the absence of such actual knowledge.

The enactment of the Insider Trading and Securities Fraud Enforcement Act ("ITSFEA") in 1988 strengthened the Securities and Exchange Commission's ("SEC") enforcement powers over insider trading and created an explicit duty for U.S. brokers dealers to establish, maintain and enforce procedures designed to control the flow on inside information. Neither the SEC nor the self regulatory organization's have promulgated regulations specifying the policies and procedures that will be deemed adequate in connection with the misuse of inside information. However, the SEC has identified several "minimum elements" necessary for the establishment of adequate procedures. Specifically, broker dealers must, among others things, (i) review customer, employee and proprietary trading through effective maintenance of some combination of watch and restricted lists, (ii) maintain a substantial Compliance Department control over relevant interdepartmental communications, and (iii) conduct heightened reviews when a firm possesses inside information.

In implementing the required policies and procedures broker dealers typically maintain a list, sometimes called a Grey List or Watch List, that includes all companies about which employees of the financial institution (for example, bankers) have knowledge of material non-public information. New companies are added to the Grey List when financial institution employees become privy to material non-public information regarding such companies. In order to add a company to the Grey List, a banker typically calls a compliance officer of the financial institution indicating that the broker dealer has, or is likely to possess inside information regarding a particular company. The Compliance Department gathers the relevant information and places the company on the Grey List in which case the employees that are involved in advising the

company are restricted from trading in the stock of the company. Furthermore, the broker dealer monitors the transactions of its employees and proprietary traders in the given company in order to detect potential misuse of the information.

In certain cases, when a financial institution's professional involvement with a company is made public, trading restrictions are imposed. For example, if the financial institution is advising Company A in its attempt to acquire Company B and the information has been made public, employees generally are restricted from trading the stock of Company A and Company B as well as engaging in any other investment or advisory activities that creates an appearance of impropriety. In addition, restrictions on proprietary trading and customer solicitation also may be imposed.

The prior art processes for managing the compliance obligations of financial institutions typically include a compliance officer of the institution that receiving from the institution's bankers information regarding the bankers' advising activities with respect to particular companies. Based on the nature of these activities and the status of any transactions contemplated by the bankers' clients, the compliance officer then places the particular companies on the Grey List, the Restricted List or no list altogether. If a particular company is placed on either the Grey List or Restricted List, then the compliance officer also includes details of the contemplated transaction such as expected timing of the deal, the composition of the deal team, the details of the transaction, etc.

Certain employees of many broker dealers are required by firm policy to pre-clear personal securities transactions. The employee must interact with the compliance officer to determine whether the trade includes a company on either the Grey List or Restricted List. If the trade includes a company on the Restricted List, then the compliance officer

indicates to the employee that the employee is prohibited from making the contemplated trade. If the trade includes a company on the Grey List, then the compliance officer will generally not prohibit the trade unless the inquiring employee is directly involved in advising the company and therefore would be in the position of knowing material non-public information regarding the company.

In addition to pre-clearing trades, the prior art compliance processes also include monitoring the trading activity of employees throughout the institution for each company on the Grey List. If the compliance officer notices an increase in trading activity in any of the companies on the Grey List, then the compliance officer may initiate an investigation to determine whether the trading activity is a result of improper use of any material non-public information.

The prior art processes used by financial institutions for monitoring trading activities for compliance with insider trader regulations have numerous shortcomings. First, the process of pre-clearing a trade typically requires the compliance officer to individually review each trade request received from employees to determine if any of the underlying companies are on the Grey List or Restricted List. This is a manually intensive and slow process resulting in two problems for financial institutions. First, this requires that financial institutions allocate scarce and precious compliance resources to a purely ministerial function, precluding the opportunity to apply those resources against higher level compliance services. Second, employees desiring to execute trades may not receive clearance in time to execute the trade at a favorable price. This problem is further exacerbated in fast-paced financial markets when waiting for a compliance officer to approve a trade is unacceptable. Maintaining a compliance program in globally dispersed

financial institutions is even more problematic because of the difficulty in providing employees a trade pre-clearance that may depend on updates to the Grey List and/or Restricted List that originates several time zones away. The inability of the prior art compliance processes to efficiently manage the Grey List and Restricted List in a global context may result, for example, in a Japanese employee executing a trade in the stock of a particular company that a New York-based banker is advising because the Restricted List has not yet been updated by the New York compliance officer who may not be available to otherwise pre-clear the trade during Japanese trading hours. Because the prior art compliance processes are inefficient and often ineffective at spotting Grey List and Restricted List trading violations, a financial institution may be subject to substantial fines for its inability to monitor and prevent trades that violate insider trading regulations.

Accordingly, it is desirable to provide a system for implementing a compliance program in a geographically-dispersed financial institution.

SUMMARY OF THE INVENTION

The present invention is directed to overcoming the drawbacks of the prior art. Under the present invention a system for implementing a compliance program in a financial institution is provided and includes a list database for storing material information regarding a plurality of entities that is known to said financial institution. Also included is a list manager that receives a compliance query from an affiliate of the financial institution having a status. The list manager provides a compliance response to the affiliate based on the plurality of entities and according to the status of the affiliate.

According to an exemplary embodiment, the material information regarding the plurality of entities is partitioned into a Grey List and a Restricted List.

According to another exemplary embodiment, the affiliate is an employee, the compliance query is a request by the employee to trade a security of an entity and the compliance response is a denial of the request to trade if the entity is included in the partition of the plurality of entities included in the Restricted List.

According to yet another exemplary embodiment, the affiliate is a trader, the compliance request is a request to trade a security of an entity and the compliance response includes at least one of the plurality of entities included in the Restricted List and a clearance code.

In still yet another exemplary embodiment, associated with the at least one of the plurality of entities is a transaction type and the request to trade has an activity type and wherein the clearance code denies the request to trade based on the transaction type and the activity type.

In an exemplary embodiment, the transaction type is selected from a group including mergers and acquisitions, initial public offerings and tender offers.

In another exemplary embodiment, the activity type is selected from a group including principal activity, market making activity, positional trading activity and derivative trading activity.

In yet another exemplary embodiment, the affiliate is a supervisory analyst, the compliance request is a request to issue a report regarding an entity and the compliance response includes at least one of the plurality of entities included in a combination of the Restricted List and the Grey List.

In still yet another exemplary embodiment, the compliance response includes at least one safe harbor provision that grants at least a portion of the compliance request.

In an exemplary embodiment, the grant of the portion of the compliance request is based on geography.

In another exemplary embodiment, the affiliate is a compliance officer, the compliance request is a request to view at least a portion of a combination of the Restricted List and the Grey list and the compliance response includes the portion of the combination of the Restricted List and the Grey List.

In yet another exemplary embodiment, the compliance response includes for at least one of the plurality of entities included in the portion a clearance code and a transaction type.

In still yet another exemplary embodiment, the compliance response includes for at least one of the plurality of entities included in the portion a safe harbor provision.

In an exemplary embodiment, a surveillance system is included that receives the plurality of entities stored in the list database for monitoring trading activity in accordance with the compliance program.

In another exemplary embodiment, the list database receives the plurality of entities from a compliance officer in communications with the system.

In yet another exemplary embodiment, the list database receives at least a portion of the plurality of entities from a transaction information source.

In still yet another exemplary embodiment, the list database receives positional information relating to the financial institution and the compliance response is based on the positional information.

In an exemplary embodiment, the list database receives affiliate directorship information and the compliance response is based on the affiliate directorship information.

Under the present invention, a method for implementing a compliance program in a financial institution is provided and includes the step of storing a plurality of entities in which the financial institution is associated with each of said plurality of entities. Next, a compliance query is received from an affiliate of the financial institution having a status. Finally, a compliance response is provided to the affiliate based on the plurality of entities and according to the status of the affiliate.

In an exemplary embodiment, the plurality of entities is partitioned into a Grey List and a Restricted List.

In another exemplary embodiment, trading activity is monitored in accordance with the compliance program based on the plurality of entities stored.

In yet another exemplary embodiment, the plurality of entities is received from a compliance officer.

In still yet another exemplary embodiment, at least a portion of said plurality of entities is received from a from a transaction information source.

In an exemplary embodiment, positional information relating to said financial institution is received and the compliance response based on the positional information is provided.

In another exemplary embodiment, affiliate directorship information is received and the compliance response based on the affiliate directorship information is provided.

Under the present invention, a system is provided for monitoring trading activity of a trading system operated by a financial institution in accordance with a compliance program wherein the trading system receives a trade request to trade a security of an entity. The system includes a list database for storing a plurality of entities wherein the financial institution is associated with each of the plurality of entities. The trading system receives the plurality of entities from the list database and allows the trade request if the entity is not included in any of the plurality of entities.

Under the present invention, a method for monitoring trading activity of a trading system operated by a financial institution in accordance with a compliance program is provided and includes the step of storing a plurality of entities wherein the financial institution is associated with each of the plurality of entities. Next, a trade request to trade a security of an entity is received. Next, it is determined whether the entity is included in the plurality of entities. Finally, the trade request is allowed if the entity is not included in the plurality of entities.

Accordingly, a method and system is provided for implementing a compliance program in a geographically-dispersed financial institution.

The invention accordingly comprises the features of construction, combination of elements and arrangement of parts that will be exemplified in the following detailed disclosure, and the scope of the invention will be indicated in the claims. Other features and advantages of the invention will be apparent from the description, the drawings and the claims.

DESCRIPTION OF THE DRAWINGS

For a fuller understanding of the invention, reference is made to the following description taken in conjunction with the accompanying drawings, in which:

FIG. 1 is a block diagram of a global compliance system of the present invention;

FIG. 2 is a screenshot of an add transaction screen included in the compliance system of FIG. 1;

FIG. 3 is a screenshot of an add issuer detail screen included in the compliance system of FIG. 1;

FIG. 4 is a screenshot of an add deal team detail screen included in the compliance system of FIG. 1;

FIG. 5 is a screenshot of a Grey List issuer detail screen included in the compliance system of FIG. 1;

FIG. 6 is a screenshot of a search transactions screen included in the compliance system of FIG. 1;

FIG. 7 is a screenshot of a query results screen included in the compliance system of FIG. 1;

FIG. 8 is a screenshot of a general view screen included in the compliance system of FIG. 1;

FIG. 9 is a screenshot of a transaction comment screen included in the compliance system of FIG. 1;

FIG. 10 is a screenshot of a deal team screen included in the compliance system of FIG. 1;

FIG. 11 is a screenshot of a trader query response screen included in the compliance system of FIG. 1;

FIG. 12 is a screenshot of a supervisory analyst search transactions screen included in the compliance system of FIG. 1;

FIG. 13 is a screenshot of a supervisory analyst query response screen included in the compliance system of FIG. 1;

FIG. 14 is a screenshot of a private bank result screen included in the compliance system of FIG. 1;

FIG. 15 is a block diagram of a global compliance system according to an exemplary embodiment of the present invention;

FIG. 16 is a block diagram of a global compliance system according to another exemplary embodiment of the present invention; and

FIG. 17 is a block diagram of a global compliance system according to yet another exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to FIG. 1, there is shown a block diagram of a global compliance system 101 of the present invention. System 101 is typically operated by a financial institution that receives material information regarding their clients and therefore must take steps to prevent its employees, traders and analysts from engaging in activities pertaining to those clients while the material information is not publicly known. In an exemplary embodiment, the material information may also include, by way of non-limiting example, employee registration status, human resources information and any other information that may be relevant to performing a compliance function. According

to an exemplary embodiment, system 101 is a computer system that executes software that performs the functions to be described below.

At the heart of system 101 is a list database 103 that contains a plurality of entities about which any of the employees (for example, bankers) of the financial institution has material non-public information. The entities contained in list database 103 are partitioned into a plurality of files including at least a restricted list file 105 that includes those entities that are on the financial institution's Restricted List and a Grey list file 107 that includes those entities that are on the financial institution's Grey List. List database 103 also includes a deal team file 109 that includes for each entity included in either restricted list file 105 or Grey list file 107 any employees of the financial institution that are a member of a team that is in possession of material non-public information pertaining to the entity.

In an exemplary embodiment, restricted list file 105, Grey list file 107 and deal team file 109 included in list database 103 are populated by a compliance officer that is affiliated with the financial institution for maintaining the financial institution's Restricted List and Grey List. To populate list database 103, the compliance officer uses a compliance officer (CO) access device 111 (for example, a personal computer) to communicate with system 101 using any known communications method and protocol, such as the Internet. CO access device 111 interfaces with a user interface 119 that provides the compliance officer with the various data entry screens to enter and maintain the Restricted List and Grey List, as will be described below. System 101 also includes a list manager that receives the compliance officer's data entry and requests from user

interface 119 and either retrieves the requested information from or causes information to be stored in list database 103, as appropriate.

Typically, the compliance officer receives from employees in the financial institution, such as bankers, the names of entities for which the employees have a relationship and therefore may be in possession of material non-public information. Generally, a banker may receive such material non-public information in the context of advising the entity with respect to a transaction, such as a merger or an initial public offering. The compliance officers determine whether any particular entity forwarded by a banker should be added to the financial institution's Grey List or Restricted List or other lists that may be maintained. If the compliance officer determines that a particular entity should be included in one of the lists, the compliance officer then determines under what circumstances should trading activity or the publication of research be allowed in the securities of that particular entity. Such a determination may be governed by policies set by the financial institution and/or government regulations as well as other business considerations. When the compliance officer receives from the financial institution employees information regarding entities that the compliance officer determines should be included in either the financial institution's Restricted List or Grey List, the compliance officer operates CO access device 111 to input this information into list database 103. Before an analyst affiliated with the financial institution issues a report regarding an entity, a supervisory analyst (SA) typically checks whether the issuing entity is on either the financial institution's Restricted List or Grey list and, if so, what restrictions have been placed on publishing research about a particular security issued by the entity. Supervisory Analysts use SA Access Device 115 to access the system 101

using any known communication protocol. SAs are given a limited read only access to Restricted List and Grey List entered by the Compliance Officers. Private Bankers access the system by using Private Bank Access Device 125 to retrieve a list of securities which are Restricted only to Private Bankers by the Compliance Officers. Some users are given a read only access to the Compliance Officer Home Page. These include people who have the rights to view the non-public information but do not have the rights to make any changes to them. They access the system using the Read Only Access Device 113. Trader Access Device 127 is used by the trader typically to check whether the security he wishes to trade on is on the financial institution's Restricted List and, if so, what restrictions have been placed on trading the particular security. Finally, Administrative Access Device 117 is given to the system administrators. This access level gives administrators the right to add new users to the system, delete deals that are not relevant, send out Restricted List emails to the concerned persons and make announcements to all the compliance officers using the system. One compliance officer per region is given administrative access to the system.

Referring now to FIG. 2, there is shown a screenshot of an add transaction screen 201 via which a compliance officer adds general information regarding an entity to be added to list database 103. Initially, the compliance officer selects in a list type field 203 the particular list – Restricted List, Grey List or Radar List – in which the entity is to be included. The compliance officer then adds additional information regarding the entity and a contemplated transaction involving the entity in various fields. For example, the compliance officer enters the name of the business group of the financial institution that is engaged with the entity into a business group field 205; the date on which the entity's

inclusion in the particular list is effective in an effective date field 207; the expected date the contemplated transaction is to take place in a transaction timing field 209; a tickler date that will be used by the compliance officers as a reminder in a tickler date field 211; the date on which the entity will be removed from the particular list in a off date field 213 and the name of the responsible compliance officer in a compliance officer field 215. Next, the compliance officer enters into a transaction type field 217 the type of transaction regarding which the financial institution is advising the entity. Such transaction types may be any type of transaction in which an entity may be engaged or any type of advisory services a financial institution may provide pertaining to the entity including, by way of non-limiting example, a merger and acquisition, an initial public offering and a tender offer. Finally, the compliance officers enters a code name into a code name field 219, a brief description of the contemplated transaction in a transaction description field 221, tickler comments (as a reminder on the ticker date) in the tickler comments field 223 and comments regarding the transaction in a transaction comments field 223.

Referring now to FIG. 3, there is shown a screenshot of an add issuer detail screen 301 into which the compliance officer enters details regarding entity transactions for entities to be included in the Restricted List. The detailed information entered into screen 301 is primarily divided into three sections: a sales and trading restrictions section 335, a research suppressions section 337 and an additional issuer information section 339. In sales and trading restrictions section 335, the compliance officer enters information that describes the extent to which salespeople and traders associated with the financial institution are restricted in trading the securities of the particular entity. For example, the

compliance officer enters a restriction code into a restriction code field 303. The restriction code indicates what activities for each transaction type involving the entity or its securities are permissible and/or prohibited. Transaction types may include, by way of non-limiting example, M&A transactions, initial public offerings and tender offers. For each transaction type, traders and salespeople may be allowed/prohibited to engage in certain activity types including, by way of non-limiting example, market making activity, principal trading activity, positional trading activity, proprietary trading activity and client solicitation. For instance, if the transaction type is M&A (i.e., the financial institution is advising the entity in an M&A transaction), then the trader may be prohibited from engaging in proprietary trading activity (trading on behalf of the financial institution). Similarly, any other transaction types and activity types may be defined and a restriction code may be designated to indicate to a trader what activity types are permissible/restricted for a given transaction type.

The compliance officer also enters into an applicable class field 305 the type of security for which the restriction applies. Finally, the compliance officer may enter any additional comments regarding the restriction in a restriction comments field 306. The information the compliance officer enters into sales and trading restrictions section 327 are provided to an inquiring trader to guide the trader's trading activities, as will be described below.

The compliance officer also enters information into research suppressions section 337 for the purpose of restricting the activities of research analysts that may be issuing a research report pertaining to an entity on the Restricted List. First, the compliance officer enters into a forecast field 307 the scope to which the financial institution analysts are

restricted from issuing a forecast regarding an entity of the Restricted List. For example, the compliance officer may select a "Global" restriction that indicates that the analysts are restricted from issuing a forecast regarding the entity anywhere in the world. In certain cases the compliance officer may only restrict an analyst from issuing a forecast about a particular entity in the United States or some other region of the world. In other cases, the compliance officer may not restrict analysts from issuing a forecast altogether. The compliance officer also enters into a Rating/Recommendation field 309 the scope to which the analysts may issue a rating/recommendation regarding the entity. For example, the compliance officer may restrict the analysts from issuing a rating recommendation globally, regionally or not at all. Next, the compliance officer will indicate in a Safe Harbor: Rule 138 field 311 and a Safe Harbor: Rule 139 field 317 whether the Rule 138 and/or Rule 139 safe harbors, respectively, apply for the particular entity. In a Research Text field 315, the compliance officer enters the geographic regions in which the analysts are restricted from issuing research text.

In addition, the compliance officer enters into a Role field 313 the role the financial institution is playing in the transaction involving the particular entity. For example, if the financial institution is a Manager/Co-Manager of an initial public offering involving the entity, then the compliance officers enters this information into Role field 313. Sensitivity level of the security is set in sensitivity field 318. The compliance officer also enters into an SA comments field 319 in research suppressions section 337 any comments appropriate for a supervisory analyst, into CO comments field 321 any comments appropriate for compliance officers and into Disclaimer Language field 323

any specific disclaimer language an analyst must include in a research report pertaining to an entity that is in the Restricted List.

Screen 301 also includes an additional user information section 339 that includes a local code field 325 for entering the Bloomberg symbol if it is not obtained from the database that contains the security details. Aka field 327 is used to enter aliases to the selected security. For example, International Business Machines is also know as IBM, International Busn Machine etc., and these aliases can be entered in aka field 327. This feature is useful as the user can search for a security using the alias names. The compliance officer selects either Private Bank, Asset Management or Private Bank Asset Management if a security has to be on the Restricted List for the Private Bankers. It is set to Not Applicable if it does not concern the Private Bankers. Market Maker is set to either Yes or No in the Market Maker field 331 and Research Coverage is set to either Yes or No in the Research Coverage field 333.

Referring now to FIG. 4, there is shown a screenshot of an add deal team detail screen 401 into which the compliance officer enters details regarding the deal team in the financial institution that is advising the particular entity regarding a transaction. Screen 401 includes fields to enter pertinent information regarding each member of the team including a role field 403 for enter the deal team member's role, a sector/product group field 404 for entering the group to which the team member belongs, an effective on date field 405 for entering the date the particular team member joined the team and a comments field 406.

Referring now to FIG. 5, there is shown a screenshot of a Grey List issuer detail screen 501 into which the compliance officer enters details regarding entities to be

included in the Grey List. In screen 501, the sensitivity level of the security is selected in the sensitivity field 503, the compliance officer enters any comments regarding the entity that is suitable for a supervisory analyst into a SA comments field 505. "No research allowed-IPO" is an example of an SA comment entered by the compliance officer that will be used as a reference by the supervisory analysts. Any comments regarding the entity that is suitable for a compliance officer is entered into a CO comments field 507, ("Watch research" is an example of the CO comment that may be entered by a Compliance Officer). In addition, a local code is entered into a local code field 509, a aka into aka field 511, a market maker into market maker field 513 and research coverage into research coverage field 515.

Referring now to FIG. 6, there is shown a screenshot of a search transactions screen 601 via which a compliance officer may search list database 103 for entities that match a particular search criteria. In the exemplary embodiment depicted in screen 601, a compliance officer may search list database 103 by selecting in a transaction status field 603 a transaction status (for e.g., Open, Closed or All), for the purpose of retrieving from list database 103 those entities that are involved in a transaction that meets the selected transaction status. The compliance officer selects in a list type field 605 the type of list that is to be searched including the Grey List, the Restricted List, the RADAR List or a combination of all of these lists. The compliance officer also selects the security search criteria by either choosing the security name search, Bloomberg symbol search, cusip code search, isin code search, sedol code search, Reuters code search or the code name search in the search criteria field 607 and enters into a security name field 608 the name of a particular entity to be searched for in list database 103. In an exemplary

embodiment, the input into security name field 608 may be a partial input and the search mechanism used may be a fuzzy search or any other search mechanism that provides search results based on a partial input. Reports Section 609 has reports that generate Active Grey Lists, Active Restricted Lists, Active Grey and Restricted Lists, Recent Grey Lists, Recent Restricted Lists and Recent Grey and Restricted Lists. Compliance officers and Supervisory Analysts have access to these reports. Tickler Comments Report is used only by the Compliance Officers. There is a section for Announcements 611 where the administrator can enter comments that will be viewed by all the compliance officers.

Referring now to FIG. 7, there is shown a screenshot of a query results screen 701 that is generated by a search request invoked by search transactions screen 601. Screen 701 displays various fields of information for each entity that meet the search criteria including a Txn ID field 703 which is a unique identifier for a particular deal, a list field 705 that indicates the list type in which the entity is included, an issuer field 707 that is the name of the entity, an aka field 709 that is the alias for the security, a transaction field 711 that indicates the transaction type regarding which the financial institution is advising the entity, a date on field 713 that is the date the entity was placed on the particular list (for the given transaction) and a date off field 715 that is the date the entity (for a particular transaction) is to be removed from the given list. In an exemplary embodiment, any other suitable information may also be displayed in results screen 701.

Referring now to FIG. 8, there is shown a screenshot of a general view screen 801 that is displayed when an entity listed in results screen 701 is selected using the txn Id (for e.g., by clicking on the entity with a computer mouse). A compliance officer may also accesses general view screen 701 by activating a general information link 813.

General view screen 801 is divided into four sections: a general information section 803 that summarizes the information the compliance officer entered via general information screen 201, an issuer information section 805 that summarizes information regarding a particular security of an entity entered via the issuer information screen 301 and also additional information retrieved from the database that stores the issuer details like the cusip, sedol, Bloomberg symbol, isin etc., a research suppressions section 807 and a sales & trading restrictions section 809 that summarizes information entered via issuer detail screen 301. In an exemplary embodiment, the compliance officer may directly edit any information contained in general view screen 801.

Referring now to FIG. 9, there is shown a screenshot of a transaction comment screen 901 that includes any comments made regarding a particular entity for a given transaction. A compliance officer accesses transaction comment screen 901 by activating an additional comment link in the general information section 803. Transaction comment screen 901 includes a comment date section 903 that lists the date, the comment author section 905 that lists the name of the author and the content section 907 that contains the comment made. A comment field 905 is included that displays the text of all the comments made by each author listed in comment author section 909. A comment entered into the comment field 909 can be submitted as either a transaction comment by clicking on submit button 913 or can be submitted as the CFD comment by clicking on the submitcfd button 911. The CFD comment is entered by the compliance officers regarding the entity that is suitable for the Corporate Finance Department.

Referring now to FIG. 10, there is shown a screenshot of a deal team screen 1001 that lists information regarding all the members of a team that is involved with advising

the entity for the particular transaction. A compliance officer may accesses deal team screen 1001 by activating a deal team link 811.

Thus, a compliance officer uses CO access device 111 to interact with system 101 for maintaining restricted list file 105, Grey list file 107 and deal team file 109 stored in list database 103.

Before a trader affiliated with the financial institution places a trade in a security issued by an entity, either for a financial institution client or on behalf of the financial institution itself, the trader is typically required to check whether the issuing entity is on the financial institution's Restricted List and, if so, what restrictions have been placed on trading the particular security. To make such a determination, the trader operates a trader access device 127 (for example, a personal computer executing suitable software) that communicates with system 101 using any known communications method and protocol, such as the Internet. Trader access device interfaces with user interface 119 for sending to list manager 121 a query from the trader regarding whether a particular entity is on the Restricted List. List manager 121 retrieves the responsive information from restricted list file 105 contained in list database 103 and forwards the information to trader access device 127 via user interface 119.

Referring now to FIG. 11, there is shown a screenshot of a trader query response screen 1101 according to an exemplary embodiment that includes at least a portion of the Restricted List that is responsive to a trader's query. Response 1101 includes a new addition section 1103 that lists entities that have been recently added to the Restricted List. For each entity included in new addition section 1103, information is provided upon which the trader can determine whether a contemplated trade is restricted. For example,

included is an issuer field 1104 that lists the name of the particular entity, a plurality of issuer ID number fields 1105 that include the ID number of the entity security that is restricted, an RL code field 1106 that indicates the restriction level set by the compliance officer (in restriction code field 303 of issuer detail screen 301) for the particular entity, a date field 1107 that indicates the date the entity was placed on the Restricted List and the date it is expected that the entity will be removed from the Restricted List guide (as provided by the compliance office via general information screen 201), a location field 1108 that indicates the location within the financial institution from which the restriction regarding the entity originated, a transaction type field 1109 that indicates the nature of the relationship between the financial institution and the entity and the type of transaction for which the financial institution is advising the entity and a comments field 1110 that provides the trader with any comments regarding the restriction that the compliance officer has inserted into restriction comments field 306 of issuer detail screen 301.

Response 1101 also includes a removed section 1111 that provides similar information as provided in new additions section 1103 for entities that have been recently removed to the Restricted List.

Based on the restriction included in RL code field 1106 (as described above), the inquiring trader determines whether contemplated transaction is restricted.

Before an analyst affiliated with the financial institution issues a report regarding an entity, a supervisory analyst (SA) typically checks whether the issuing entity is on either the financial institution's Restricted List or Grey List and, if so, what restrictions have been placed on publishing research about a particular security issued by the entity. To make such a determination, the SA operates an SA access device 115 (for example, a

personal computer executing suitable software) that communicates with system 101 using any known communications method and protocol, such as the Internet. SA access device interfaces with user interface 119 for sending to list manager 121 a query from the SA regarding whether a particular entity is on either the Restricted List or Grey List. List manager 121 retrieves the responsive information from restricted list file 105 and Grey list file 107 contained in list database 103 and forwards the information to SA access device 115 via user interface 119.

Referring now to FIG. 12, there is shown a screenshot of a supervisory analyst home page screen 1201. In the exemplary embodiment depicted in screen 1201, the supervisory analyst selects in a list type field 1203 the type of list that is to be searched including the Grey List, the Restricted List or a combination of all of these lists. The SA also selects the security search criteria by either choosing the security name search, Bloomberg symbol search, cusip code search, isin code search, sedol code search, Reuters code search or the code name search in the search criteria field 1205 and enters into a security name field 1207 the name of a particular entity to be searched for in list database 103. In an exemplary embodiment the input into security name field 1207 may be a partial input and the search mechanism used may be a fuzzy search or any other search mechanism that provides search results based on a partial input if the exact match section 1209 is not checked -- otherwise it retrieves the exact search criteria results. Reports Section 609 has reports that generate Active Grey Lists, Active Restricted Lists, Active Grey and Restricted Lists, Recent Grey Lists, Recent Restricted Lists and Recent Grey and Restricted Lists. Last Update Section 1211 displays the date and time of the

latest addition of Grey or Restricted List made to the system by the Compliance Officer and is used as a reference by the supervisory analysts.

Referring now to FIG. 13, there is shown a screenshot of a supervisory analyst query response screen 1301 according to an exemplary embodiment that includes at least a portion of the Restricted List and Grey List that is responsive to an SA's query. Response 1301. For each entity included in search results section 1323, information is provided upon which the SA can determine whether the publication of a particular research report is permissible. For example, included is an issuer field 1307 that lists the name of the particular entity, a plurality of issuer ID number fields 1309 that include the ID number of the entity security that is restricted, a date field 1311 that indicates the date the entity was placed on the particular list and the date it is expected that the entity will be removed from the list and a location field 1208 that indicates the location within the financial institution from which the entry regarding the entity originated. Also included is a list field 1303, a sensitivity level field 1305, a safe harbor field 1315 that correspond to fields in research suppression section 329 of issuer detail screen 301 in which the compliance officer indicates under what circumstances an analysts report regarding the entity may be published, as described above. In an exemplary embodiment, other fields may be included such as a field displaying any comments from the compliance officer regarding the entity, the names of deal team members who are over the wall as in field 1317 and the transaction type as in field 1319. A query section 1321 is included for an easier search functionality for the users.

Referring to FIG. 14, there is shown a screenshot of a private bank query response screen 1401. In the exemplary embodiment depicted in screen 1401, the private

banker is given access to all the securities that is Restricted for the private bankers by the Compliance Officers. Screen 1401 displays various fields of information for each entity including an issuer field and aka field 1403 that is the name of the entity and its alias, a date field 1405 that is the date the entity was placed on the particular list (for the given transaction) and the date the entity (for a particular transaction) is to be removed from the given list, ,the plurality of issuer ID number fields 1407 that include the ID number of the entity security that is restricted, the country section 1409 for that security, the name of the compliance officer who entered the deal in the section 1411, a transaction field 1413 that indicates the transaction type regarding which the financial institution is advising the entity and a Restriction field 1415 that displays the restriction on that security. In an exemplary embodiment, any other suitable information may also be displayed in results screen 701.

As with a query provided to system 101 by a trader, a query provided by an SA may include all or party of the name of a particular entity in which case Response 1201 will include those entities that match the provided search phrase. Also, it will be obvious to provide the SA with a mechanism for searching on other fields contained in restricted file list 105 and Grey list file 107.

Typically, before an employee of a financial institution is allowed to transact in a security in the employee's personal account, the employee is required to check whether the entity issuing the security is on the financial institution's Restricted List. To make such a determination, the employee operates an employee access device (for example, a personal computer executing suitable software) that communicates with system 101 using any known communications method and protocol, such as the Internet. Employee access

device interfaces with user interface 119 for sending to list manager 121 a query from the employee as to whether the contemplated transaction is prohibited based on the Restricted List contained in restricted list file 105. Based on the information contained in restricted list file 105, list manager 121 determines whether the employee transaction is permissible and forwards the response to employee access device 117 via user interface 119.

Accordingly, the present invention provides a system and method for implementing a compliance program in a geographically-dispersed financial institution. Because the financial institution's Restricted List and Grey List are centrally stored in list database 103 and accessible using any known communications method and protocol, such as the Internet, any affiliate of the financial institution, such as a trader, SA and employee, may access system 101 in order to determine whether a contemplated action is allowed based on the contents of the Restricted List and Grey List and the financial institutions compliance program. In this way, a compliance officer need not be contacted by a requesting affiliate in order to approve each contemplated transaction thereby significantly increasing the rate at which contemplated transactions are approved. Furthermore, because system 101 may structured to be globally-accessible (for example, if system 101 is connected to the Internet), information entered into system 101 by a financial institution's compliance officer located in a first time zone becomes immediately accessible by affiliates of the financial institution located in a second time zone. Thus, contemplated trades or research report publications may be approved immediately without having to directly query a responsible compliance officer that may be difficult to reach.

System 101 also includes an export interface 123 that receives list information from list database 103 via list manager 121 for export to external systems. In an exemplary embodiment, export interface 123 exports to external market data systems the entities included in the financial institution's Restricted List so that securities issued by such entities that are displayed in such market systems can be labeled as a restricted securities. An example of such an external market data system is a Bloomberg system that receives the restricted list information from export interface 123 and labels the securities it displays as restricted, where appropriate, so that affiliates of the financial institution that use the Bloomberg system can see at a glance what securities are restricted.

Export interface 123 also exports Restricted List and Grey list information to a surveillance systems that is operated by the financial institution to determine that trades performed by traders and employees of the financial institution do not violate the financial institution's compliance program. Surveillance system monitors trades executed through the financial institution's trading systems and determines whether any trades involves securities of entities that are included in the Restricted List and whether the particular trade was permissible based on the scope of the restriction associated with such entities. The surveillance system also determines whether any trades involve securities of entities that are on the Grey List and, if so, is there a trading pattern in such securities that may indicate a violation of the financial institution's compliance program. In either case, the surveillance system may also notify a compliance officer of trades and trading patterns that may be impermissible and that therefore merit further scrutiny.

Referring now to FIG. 15, there is shown a block diagram of a global compliance system 1501 according to an exemplary embodiment of the present invention. Elements that are similar to elements of system 101 of FIG. 1 are identically labeled and a detailed description thereof is omitted.

System 1501 includes an input interface 1509 that receives information from three sources: a positional information source 1503, a transaction information source 1505 and a directorship information source 1507. Positional information source 1503 includes the securities in which the financial institution maintains a position that is at the financial institution's position limit for that security. Typically, positional information is derived from analyzing information from several sources including, for example, all the financial institution's trading systems and the financial institution's books and records. Once it is determined in which securities the financial institution has reached its position limits, this information is fed to system 1501 in the form of positional information source 1503. This information is then forwarded by input interface 1509 to list manager 121 that determines the entities that should be restricted based on the position limits reached by the financial institution. List manager 121 then causes such restrictions to be stored in restricted list file 105 contained in list database 103.

Transaction information source 1505 includes information regarding the transactions the financial institution's bankers are engaged in. This information may be derived from systems in that are used by the financial institution's bankers to document each ongoing transaction. Based on this information, list manager 121 determines those entities that are included in any of the transactions and that therefore should be included in either the Restricted List or Grey List and under what circumstances should trading

and research publication be restricted. List manager 121 then causes such restrictions to be stored in restricted list file 105 contained in list database 103.

Directorship information source 1507 includes information regarding the directorships any financial institution affiliates maintain that may give rise to a trading/publication restriction. Based on this information, list manager 121 determines those entities that for which an affiliate holds a directorship and that therefore should be included in either the Restricted List or Grey List and under what circumstances should trading and research publication be restricted. List manager 121 then causes such restrictions to be stored in restricted list file 105 contained in list database 103.

Thus, while in system 101, a compliance officer was responsible for inputting list information into system 101, in system 1501, such information is automatically received from positional information source 1503, transaction information source 1505 and directorship information source 1507 and stored in list database 103. In addition to automatically receiving such information, a compliance officer may operate CO access device 111 to input additional compliance information or modify existing compliance information.

Referring now to FIG. 16, there is shown a block diagram of a global compliance system 1601 according to another exemplary embodiment of the present invention. Elements that are similar to elements of system 1501 of FIG. 15 are identically labeled and a detailed description thereof is omitted.

In system 1601, export interface 123 also exports Restricted List and Grey List information to the financial institution's trading system 1511. In this embodiment, trading system 1511 monitors the entities that are contained in the Restricted List and

either flag or prevent trading in securities issued by such entities that violate any restrictions contained in the list. In addition, system 1601 monitors trading patterns in securities included in the Grey List to determine whether any such patterns is in violation of the financial institution's compliance program. In either case, trading system 1511 may alert a compliance officer of any such trades or trading patterns for further investigation.

Accordingly, system 1601 automates the process by which information is received for inclusion in either the Restricted List or Grey List thereby reducing any dependence on compliance officers to gather and input such information.

Referring now to FIG. 17, there is shown a block diagram of a global compliance system 1701 according to yet another exemplary embodiment of the present invention. Elements that are similar to elements of system 1601 of FIG. 16 are identically labeled and a detailed description thereof is omitted.

In system 1701, input interface 1509 also receives information from trading systems 1511 upon which further refinement can be made to the information contained in either the Restricted List or Grey List.

Based on the above description, it will be obvious to one of ordinary skill to implement the system and methods of the present invention in one or more computer programs that are executable on a programmable system including at least one programmable processor coupled to receive data and instructions from, and to transmit data and instructions to, a data storage system, at least one input device, and at least one output device. Each computer program may be implemented in a high-level procedural or object-oriented programming language, or in assembly or machine language if desired;

and in any case, the language may be a compiled or interpreted language. Suitable processors include, by way of example, both general and special purpose microprocessors. Furthermore, alternate embodiments of the invention that implement the system in hardware, firmware or a combination of both hardware and software, as well as distributing modules and/or data in a different fashion will be apparent to those skilled in the art and are also within the scope of the invention. In addition, it will be obvious to one of ordinary skill to use a conventional database management system such as, by way of non-limiting example, Sybase, Oracle and DB2, as a platform for implementing the present invention.

It will thus be seen that the objects set forth above, among those made apparent from the preceding description, are efficiently attained and, since certain changes may be made in carrying out the above process, in a described product, and in the construction set forth without departing from the spirit and scope of the invention, it is intended that all matter contained in the above description shown in the accompanying drawing shall be interpreted as illustrative and not in a limiting sense.

It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention herein described, and all statements of the scope of the invention, which, as a matter of language, might be said to fall therebetween.